What is Claimed is:

1. A method of administering a countermeasure for a computer security threat to a computer system, comprising:

establishing a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV);

receiving a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level; and

processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

2. A method according to Claim 1:

wherein the receiving comprises receiving a TMV history file in response to installation, configuration or maintenance of the computer system; and

wherein the processing comprises processing countermeasures that are identified in the TMV history file.

3. A method according to Claim 2 further comprising updating a threat management information base for the computer system to account for the countermeasures that are processed.

4. A method according to Claim 1 wherein the processing comprises:

determining whether the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat;

adding at least one instance identifier to the TMV to account for multiple instances of the operating system running on the computer system, if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat; and

processing countermeasures that are identified in the TMV for the instance of the operating system type and operating system release level when the instance of the operating system type and operating system release level is instantiated in the computer system.

5. A method according to Claim 1 wherein the processing comprises installing and running the countermeasure.

6. A method according to Claim 1:

wherein the receiving comprises receiving a TMV including therein the first field that provides identification of at least one operating system type that is affected by a computer security threat, the second field that provides identification of an operating system release level for the operating system type, a fourth field that provides identification of at least one application program type that is affected by the computer security threat and a fifth field that provides identification of a release level for the application program type, the third field providing identification of a set of possible countermeasures for the application program type and the application program release level; and

wherein the processing comprises processing countermeasures that are identified in the TMV if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat.

7. A method according to Claim 6 wherein the processing further comprises:

determining whether the TMV identifies the application program type and application programming release level for the computer system as being affected by the computer security threat;

adding at least one instance identifier to the TMV to account for multiple instances of the application program running on the computer system if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat; and

processing countermeasures that are identified in the TMV for the instance of the application program type and application program release level when the instance of the application program type and application program release level is instantiated in the computer system.

8. A method according to Claim 1 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

9. A method according to Claim 1 wherein the receiving comprises pruning at least some of the TMV to discard at least some of the TMV that is not needed for processing countermeasures.

10. A method according to Claim 1 wherein the receiving comprises mutating the TMV that is received to a format that is compatible with processing countermeasures.

11. A computer system, comprising:

a Threat Management Information Base (TMIB) that is configured to establish a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector

(TMV);

a TMV receiver that is configured to receive a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level; and

a remediation manager that is configured to process countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

12. A system according to Claim 11 further comprising:

a TMIB configurator that is configured to receive a TMV history file in response to installation, configuration or maintenance of the computer system and to process countermeasures that are identified in the TMV history file.

13. A system according to Claim 12 wherein the TMIB configurator is further configured to update the TMIB to account for the countermeasures that are processed.

14. A system according to Claim 11 further comprising:

a TMV inductor that is configured to determine whether the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat and to add at least one instance identifier to the TMV to account for multiple instances of the operating system running on the computer system, if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat; and wherein the remediation manager is further configured to process countermeasures that are identified in the TMV for the instance of the operating system type and operating system release level when the instance of the operating system type and operating system release level is instantiated in the computer system.

15. A system according to Claim 11 wherein the remediation manager is configured to process countermeasures that are identified in the TMV by installing and running the countermeasure.

16. A system according to Claim 11:

wherein the TMV receiver is further configured to receive a TMV including therein the first field that provides identification of at least one operating system type that is affected by a computer security threat, the second field that provides identification of an operating system release level for the operating system type, a fourth field that provides identification of at least one application program type that is affected by the computer security threat and a fifth field that provides identification of a release level for the application program type, the third field providing identification of a set of possible countermeasures for the application program type and the application program release level; and

wherein the remediation manager is further configured to process countermeasures that are identified in the TMV if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat.

17. A system according to Claim 16 further comprising:

a TMV inductor that is configured to determine whether the TMV identifies the application program type and application programming release level for the computer system as being affected by the computer security threat and to add at least one instance identifier to the TMV to account for multiple instances of the application program running on the computer system if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat; and

wherein the remediation manager is further configured to process countermeasures that are identified in the TMV for the instance of the application program type and application program release level when the instance of the application program type and application program release level is instantiated in the computer system.

18. A system according to Claim 17 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

19. A system according to Claim 18 wherein the TMV receiver is further configured to prune at least some of the TMV that is not needed by the remediation manager.

20. A system according to Claim 11 wherein the TMV receiver is further configured to mutate the received TMV to a format that is compatible with the remediation manager.

21. A computer program product is configured to administer a countermeasure for a computer security threat to a computer system, the computer program product comprising a computer usable storage medium having computer-readable program code embodied in the medium, the computer-readable program code comprising:

computer-readable program code that is configured to establish a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV);

computer-readable program code that is configured to receive a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level; and

computer-readable program code that is configured to process countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

22. A computer program product according to Claim 21 wherein the computer-readable program code that is configured to process comprises:

computer-readable program code that is configured to determine whether the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat;

computer-readable program code that is configured to add at least one instance identifier to the TMV to account for multiple instances of the operating system running on the computer system if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat; and

computer-readable program code that is configured to process countermeasures that are identified in the TMV for the instance of the operating system type and operating system release level when the instance of the operating system type and operating system release level is instantiated in the computer system.